

**2025**

**中国信通院数据安全管理能力认证（DSMC）**

**专项申请表**

|  |  |
| --- | --- |
| 单位全称 |  |
| 联系地址 |  |
| 申请内容 | 数据安全管理能力认证（DSMC）  |
| 项目对接人 |  | 对接人手机 |  |
| 对接人职务 |  | 对接人邮箱 |  |
| 企业基础信息 | 所属行业 |  |
| 主营业务简述 |  |
| 行业地位 | □ 领导者 □ 有远见者 □ 挑战者  |
| 数据安全负责人（姓名、职务） |  | 负责人电话 |  |
| 计划项目启动时间 | 2024年3月 |
| 已获得认证资质 | 列举曾经获得的数据安全、网络安全相关认证资质 |
| 简述本单位当前数据安全能力建设情况（组织人员、管理制度、技术能力、监管检查要求等） |   |
| 监管处罚记录 | 如有，请详细说明处罚事由以及整改结果 |
|   公司盖章 或 数据安全负责人签字填表日期 2024年 月 日  |

请将申请表盖章扫描件传至邮箱：zxbigdata@caict.ac.cn

**数据安全管理能力（DSMC）简介**

数据安全管理能力认证（DSMC）是由中国信息通信研究院顺应数据安全法、个人信息保护法要求，面向全行业发起的数据安全领域的权威国家级认证。

### **认证依据**

《数据安全法》、《个人信息保护法》、《工业和信息化领域数据安全管理办法（试行）》、《网络数据安全管理条例（征求意见稿）》、GB/T35273-2020、GB/T 37988-2019、GB/T 36073-2018、GB/T41479-2022、GB/T 39335-2020等相关法律法规、政策、标准。认证依据随行业主管部门要求以半年度进行更新迭代。

### **认证体系**

数据安全管理能力认证从数据安全管理能力要求、技术能力要求两大维度共计15项指标进行评估，结合评估结果及组织框架要求开展认证，确保企业数据安全管理能力和技术能力满足法规要求。



中国信通院将从两大维度共计 15 项指标进行评估。具体如下：

* ****制度落地要求****：包括组织建设、制度保障、数据资产、数据审批、管理审计、合作方管理、教育培训、举报投诉、应急响应、合规性评估。
* ****技术落地要求****：包括数据识别、操作审计、数据防泄漏、接口安全管理、敏感数据保护。

### **认证流程**

DSMC管理体系主要包含以下四个阶段，这四个阶段将确定项目范围与组织架构，开展现状调研并输出差距分析报告和数据安全管理体系框架，最终形成数据安全管理体系并完成认证。



### **什么企业适用于DSMC认证**

* **合规需求较强的行业**

金融、医疗、能源、交通等敏感行业由于合规要求较为严格，通过认证完善数据安全管理能力和技术能力是企业合规的重要手段。

* **重要、中大型数据处理者**

所处理的数据涉及到国家核心数据或重要数据的，或拥有超过100万以上个人信息的中大型数据处理者。一旦数据泄露且未尽合规义务，企业有可能面临极大的经济损失甚至刑事责任风险。

* **有数据安全能力资质需求的企业**

合规要求企业在选择数据合作方时，有义务对合作方的数据安全管理能力进行审核并建立准入制度。当前，越来越多的政府机构、央企国企以及大型私营企业等已经把合作方的数据安全能力作为重要的考核依据。

* **希望建立完善的数据安全合规体系的企业**

获得DSMC认证后，一方面代表权威机构对企业保护用户隐私以及数据安全能力的认可，另一方面也展现了对企业责任的重视，以及在合规经营方面的成效。特别是针对C端服务的企业。

### **哪些领域和企业已获得DSMC认证**

截止2024年12月，来自金融科技、证券、医疗健康、游戏、物流、汽车制造、大数据、智能家居、人工智能、酒店、医美、互联网金融、营销、网络招聘、智能制造、在线教育、电商、云服务、能源、影视传媒、出行、知识付费、征信、保险等数十个领域超过100家企业获得了DSMC认证。



通过认证企业将颁发“数据安全管理能力”认证证书，认证结果可在国家认证认可监督管理委员会官方网站查询。数据安全管理能力认证(DSMC）正式开启2025年度报名。企业可点击“阅读原文”下载报名表，填写后发送至邮箱zxbigdata@caict.ac.cn。